Listing of the Claims

1. (currently amended) A method for ~~generating identification data~~ authorizing a transcation, comprising the steps of:

~~providing~~ storing an automatic teller machine (ATM) personal identification number (PIN) related to a first transaction type that is an ATM transaction, wherein said ATM PIN is associated with a corresponding customer account number;

storing a conversion key for use in performing at least one cryptographic operation;

~~and~~ generating a non-ATM electronic commerce PIN on a central computer by performing a cryptographic operation on said ATM PIN using at least said conversion key;

receiving said customer account number and said non-ATM electronic commerce PIN during an electronic commerce transaction conducted over a network, wherein said electronic commerce transaction is a non-ATM financial transaction;

performing a second cryptographic operation on said non-ATM electronic commerce PIN using at least said conversion key;

comparing the result of the second cryptographic operation to said ATM PIN; and

authorizing said electronic commerce transaction.

~~said non-ATM electronic commerce PIN to be entered by a user in a second transaction type that is a non-ATM financial transaction; and~~

~~transmitting said non-ATM electronic commerce PIN to said user.~~

2. (cancelled)

3. (currently amended) A method according to claim ~~2~~ 1, wherein the step of ~~providing~~ storing a conversion key comprises:

providing conversion key derivation data;

providing a conversion key derivation key; and

performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key.

4. (original) A method according to claim 3, wherein the step of performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises using the conversion key derivation key to perform at least one cryptographic operation upon the conversion key derivation data.

5. (original) A method according to claim 4, wherein the conversion key derivation data includes an identification number that is associated with multiple accounts, and wherein at least one cryptographic operation using a secret key is performed to cryptographically process said conversion key derivation data to produce the conversion key.

6. (previously presented) A method according to claim 1, wherein the step of performing a cryptographic operation comprises:

providing cryptographically-computed data; and

performing an operation upon the ATM PIN and the cryptographically-computed data.

7. (previously presented) A method according to claim 6, wherein the step of providing cryptographically- computed data comprises:

providing initial data; and

performing at least one cryptographic operation using a secret key upon the initial data, thereby producing the cryptographically-computed data.

8. (original) A method according to claim 7, wherein said at least one cryptographic operation using a secret key comprises at least one of a DES-encryption and a DES-decryption.

9. (original) A method according to claim 8, wherein at least a portion of the initial data is obtained from at least a portion of an account number.

10. (previously presented) A method according to claim 9, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

11. (previously presented) A method according to claim 10, wherein the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

12. (previously presented) A method according to claim 6, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

13. (previously presented) A method according to claim 6, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

14-16. (previously withdrawn)

17. (currently amended) A system for ~~generating identification data~~ authorizing a transaction, comprising:

a memory for storing an automatic teller machine (ATM) personal identification number (PIN);

wherein said ATM PIN is associated with a corresponding customer account number;

memory for storing a conversion key for use in performing at least one cryptographic operation;

a processor on a central computer for performing a cryptographic operation upon the ATM PIN, such that said processor generates a second non-ATM PIN related to a non-ATM electronic transaction ~~during which transaction a user enters said second non-ATM PIN~~; and

~~a transmission means for transmitting said non-ATM PIN to said user~~.

a memory for storing said customer account number and said non-ATM electronic commerce PIN received during an electronic commerce transaction conducted over a network, wherein said electronic commerce transaction is a non-ATM financial transaction;

a processor for performing a second cryptographic operation on said non-ATM electronic commerce PIN using at least said conversion key, comparing the result of the second cryptographic operation to said ATM PIN, and authorizing said electronic commerce transaction.

18. (cancelled)

19. (currently amended) The system of claim ~~18~~ 17, wherein the memory further includes:

means for storing conversion key derivation data; and

means for storing a conversion key derivation key; and

wherein the processor comprises means to perform a cryptographic operation upon the conversion key derivation data and the conversion key derivation key, thereby generating the conversion key.

20. (original) The system of claim 19, wherein the cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises at least one DES operation.

21. (original) The system of claim 20, wherein the conversion key derivation data is derived from an identification number, and wherein said at least one DES operation comprises:

using a portion of the conversion key derivation key to DES-encrypt the conversion key derivation data, thereby producing a first conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the first conversion key generation result, thereby producing a second conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the second conversion key generation result, thereby producing a third conversion key generation result;

using the third conversion key generation result as a first portion of the conversion key;

using a portion of the conversion key derivation key to DES-encrypt the third conversion key generation result, thereby producing a fourth conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the fourth conversion key generation result, thereby producing a fifth conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the fifth conversion key generation result, thereby producing a sixth conversion key generation result; and

using the sixth conversion key generation result as a second portion of the conversion key.

22. (previously presented) The system of claim 17, wherein the memory includes means for storing cryptographically-computed data, and wherein the processor comprises:

means for generating the cryptographically-computed data; and

means for performing an operation upon the ATM PIN and the cryptographically-computed data.

23. (original) The system of claim 22, wherein the memory further includes means for storing initial data, and wherein the means for generating the cryptographically-computed data comprises means for performing at least one cryptographic operation upon the initial data, thereby producing the cryptographically-computed data.

24. (original) The system of claim 23, wherein said at least one cryptographic operation comprises at least one of a DES-encryption and a DES-decryption.

25. (original) The system of claim 24, wherein the initial data is obtained from an account number, wherein the memory further includes means for storing a conversion key, and wherein the cryptographic operation uses the initial data and the conversion key to produce the cryptographically-computed data.

26. (previously presented) The system of claim 25, wherein the means for performing an operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction means or an addition means.

27. (previously presented) The system of claim 25, wherein the means for performing an operation further comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

28. (previously presented) The system of claim 22, wherein the means for performing an operation comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

29. (original) The system of claim 22, wherein the means for performing an operation comprises either a subtraction means or an addition means.

30-32. (previously withdrawn)

33. (currently amended) A system for ~~generating identification data~~ authorizing a transaction, comprising:

a memory on a central computer;

a processor on said central computer in communication with the memory;

a computer-readable medium on said central computer in communication with the processor and storing instructions which, when executed, cause the processor to perform the steps of:

storing in said memory an automatic teller machine (ATM) personal identification number (PIN) related to a first transaction type that is an ATM transaction, wherein said ATM PIN is associated with a corresponding customer account number;

storing in said memory a conversion key for use in performing at least one cryptographic operation;

performing a cryptographic operation upon the ATM PIN, using at least said conversion key ~~thereby generating a second PIN to be entered by a user during a non-ATM electronic transaction~~; and

~~means for transmitting said non-ATM PIN to said user.~~

receiving said customer account number and said non-ATM electronic commerce PIN during an electronic commerce transaction conducted over a network, wherein said electronic commerce transaction is a non-ATM financial transaction;

performing a second cryptographic operation on said non-ATM electronic commerce PIN using at least said conversion key;

comparing the result of the second cryptographic operation to said ATM PIN; and

authorizing said electronic commerce transaction.

34. (cancelled)

35. (currently amended) The system of claim ~~34~~ 33, wherein the ~~step of providing~~ storing a conversion key comprises:

storing conversion key derivation data in the memory;

storing a conversion key derivation key in the memory; and

performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key.

36. (original) The system of claim 35, wherein the step of performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key

comprises using the conversion key derivation key to perform at least one DES operation upon the conversion key derivation data.

37. (original) The system of claim 36, wherein the conversion key derivation data is derived from an identification number, and wherein said at least one DES operation comprises:

using a portion of the conversion key derivation key to DES-encrypt the conversion key derivation data, thereby producing a first conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the first conversion key generation result, thereby producing a second conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the second conversion key generation result, thereby producing a third conversion key generation result;

using the third conversion key generation result as a first portion of the conversion key;

using a portion of the conversion key derivation key to DES-encrypt the third conversion key generation result, thereby producing a fourth conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the fourth conversion key generation result, thereby producing a fifth conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the fifth conversion key generation result, thereby producing a sixth conversion key generation result; and

using the sixth conversion key generation result as a second portion of the conversion key.

38. (previously presented) The system of claim 33, wherein the step of performing a cryptographic operation comprises:

providing cryptographically-computed data;

storing the cryptographically-computed data in the memory; and

performing an operation upon the ATM PIN and the cryptographically-computed data.

39. (original) The system of claim 38, wherein the step of providing cryptographically-computed data comprises:

storing initial data in the memory; and

performing at least one cryptographic operation using a secret key upon the initial data, thereby producing the cryptographically-computed data.

40. (original) The system of claim 39, wherein said at least one cryptographic operation using a secret key comprises at least one of a DES-encryption and a DES-decryption.

41. (previously presented) The system of claim 40, wherein at least a portion of the initial data is obtained from at least a portion of an account number.

42. (previously presented) The system of claim 41, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

43. (previously presented) The system of claim 42, wherein the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein

said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

44. (currently amended) The system of claim 38, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing ATM PIN.

45. (previously presented) The system of claim 38, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

46-48. (previously withdrawn)

49. (previously presented) A method for generating identification data for a non-ATM electronic financial transaction over a communications network, comprising the steps of:

providing a first set of identification data related to a first transaction type;

generating a second set of identification data on a central computer by performing a cryptographic operation on said first set of identification data, wherein said first set of identification data is an ATM PIN, said first transaction type is an ATM-transaction, said second set of identification data is a non-ATM electronic commerce PIN to be entered by a user in a non-ATM electronic financial transaction; and

transmitting said non-ATM electronic commerce PIN to said user.

50. (previously presented) The method of claim 49, further comprising the step of:

performing a second cryptographic operation upon said electronic commerce PIN to generate said ATM-PIN.